Opinnäytetyö AMK

Tietojenkäsittely

Tietoverkot ja tietoturva

2017

Rasmus Kyyhkynen

KOTIVERKON IOT-LAITTEIDEN TIETOTURVA

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ AMK | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Tietoverkot ja tietoturva

2017 | 29

Rasmus Kyyhkynen

KOTIVERKON IOT-LAITTEIDEN TIETOTURVA

Tämä opinnäytetyö käsittelee esineiden internetin (IoT) tietoturvaa kotiverkossa. Työssä on kartoitettu eri tapoja IoT-järjestelmän turvaamiseksi. Työssä tarkasteltiin sovelluksien ja laitteiden tietoturvamenetelmiä, jotka estävät laitteiden luvattoman käytön tai datan varastamisen.

Opinnäytetyön teoriaosuus muodostuu esineiden internet -käsitteiden avaamisesta ja kuinka esineiden internet -järjestelmistä saadaan tietoturvallinen. Esineiden internet -laitteet ovat tavallisia laitteita tai esineitä, joihin lisätään älyä. Laitteisiin lisättävällä älyllä tarkoitetaan, että laitteeseen lisätään mahdollisuus kytkeä laite verkkoon ja antureita keräämään tietoa. Huolellisella IoT-laitteen suunnittelulla ja verkon monitorointia käyttäen saadaan kotiverkosta tietoturvallinen. Tietoturvamenetelmien lähteenä on käytetty Open Web Application Security Project (OWASP) Internet of Things -projektia, IBM:n laatimaa artikkelia esineiden tietoturvasta ja miten se kuuluisi hoitaa sekä Teollinen internet -kirjaa.

Työn lopputuloksena on ohjeistus IoT-laitteiden ja sovelluksien tietoturvan parantamiseksi ja ehdotuksia ohjelmista ja laitteista, joilla IoT-tietoturvaa pystyy parantamaan kotiverkossa. IoT-laitteet tulisi suunnitella huolellisesti tietoturvan kannalta. Suunnitteluun kuuluu tietoturvallinen laiteohjelmisto, laitekommunikaation salaus, taustaohjelmistojen tietoturva ja hyvä laitteiden sekä käyttäjien todennus. IoT-laitteiden tietoturvaa kotiverkossa pystyy parantamaan erillisellä tietoturvalaitteella, joka aktiivisesti monitoroi tietoliikennettä.

Suurimmilla yrityksillä, kuten IBM:llä ja Microsoftilla, on ohjelmistot ja laitteet, joilla esineiden internet -järjestelmistä saadaan tietoturvallisia. Yrityksien IoT-pilvipalvelusovelluksien tietoturva on otettu vakavasti ja niihin on integroitu tietoturvaa parantavia menetelmiä. Markkinoilla olevia palomuureja on mahdollisuus integroida IoT-järjestelmiin. Yksityisten käyttöön ei ole vielä tullut laitteita tai ohjelmistoja, joilla IoT-järjestelmästä saisi tietoturvallisen. Bitdefender-tietoturvatalolla on IoT-laitteiden tietoturvaa parantava laite ja ohjelmistopaketti, jolla tietoturvaa kotiverkossa pystyy parantamaan. F-Secure on tuomassa Sense-paketin, jolla IoT-tietoturvaa pystyy parantamaan pilvessä toimivan verkkoliikenteen monitoroinnin avulla.

ASIASANAT:

tietoturva, esineiden internet, teollinen internet

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Business Data Communications and Information Security

2017 | 29

Rasmus Kyyhkynen

IOT DEVICE'S INFORMATION SECURITY IN HOME NETWORK

The purpose of this thesis was how to make Internet of Things more secure at home. In this thesis, there are theoretical methods to make IoT systems more secure in software and in devices that make those things more secure so that nobody can use IoT devices without authorization or steal any data.

Theoretical part of this thesis consists of Internet of Things concepts and how to make IoT systems secure. Internet of Things device is a normal device or thing where intelligence is added in device. The purpose of added intelligence is to put device or thing in network and add sensors in it. With careful designing of IoT device and network monitoring can home network be secure. Information security methods are from Open Web Application Security Project (OWASP) Internet of Thigs project, IBM's article about what IoT security is and how to make IoT systems secure and from the "Teollinen internet" book.

Outcome of this thesis is indicative guide to make IoT devices and applications secure in home network in general and how to increase information security with security companies' products. Second outcome of this thesis is proposal of software and devices that make IoT systems more secure in home network. IoT devices should be designed carefully. Designing of IoT systems should consist of secure firmware, secure device communication, secure backend software and good device and user authentication. IoT device's information security in home network can be improved with active network monitoring device.

Biggest companies like IBM and Microsoft have software and devices that secure IoT systems. Both companies have IoT cloud software. Security has been one point of view when these tools have been made. Firewalls that are in markets can be integrated in IoT systems. For private use, there aren't many devices or software that can make IoT system more secure. Bitdefender information security company has product that consists of device and software that increase information security in home network. F-Secure is bringing device and software combination Sense that can make systems more secure with cloud software that monitors network traffic.

KEYWORDS:

Information security, internet of things, industrial internet of things

SISÄLTÖ

KUVAT

KÄYTETYT LYHENTEET TAI SANASTO

anomalia	poikkeama normaalista
autentikointi	käyttäjän tunnistaminen ja todentaminen
DDoS	palvelunestohyökkäys, Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DLP	Data Leak Prevention tai Data Loss Prevention
IoT	esineiden internet, Internet of Things
IIoT	Industrial Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
NIDS	Network Intrusion Detection System
OWASP	The Open Web Application Security Project
RFID	Radio-Frequency Identification
TLS	yhteyden salaus, Transport Layer Security
URL	WWW -verkko-osoite, Uniform Resource Locator
VPN	yhteyden salaus tunnellin avulla, Virtual Private Network
WiFi	kaupallinen nimitys langattomalle verkolle
WLAN	langaton verkko, Wireless Local Area Network
2G	langaton mobiiliverkko, Second Generation
3G	langaton mobiiliverkko, Third Generation
4G LTE	langaton mobiiliverkko, Fourth Generation Long Term Evolution
5G	langaton mobiiliverkko, Fifth Generation
6LoWPAN	IPv6 over Low power Wireless Personal Area Network

1 JOHDANTO

Tietoturva aiheena on hyvin ajankohtainen digitalisoituvassa maailmassa. Media uutisoi kyberuhista ja tietoturvahakkereista, jotka anastavat tietoa isojen yrityksien palvelimilta ja jakavat niitä internetissä kaikille saataville.

Maiden välistä kyberuhkaa on koko ajan, mutta sitä ei tavallinen ihminen pysty tiedostamaan. Maiden välillä hyökätään ja toinen maa yrittää toiselta maalta urkkia tietoa, niin sähköpostiliikennettä kuin kaikkea muuta internetliikennettä. (Norse 2016.)

Palvelunestohyökkäykset ovat myös yleisiä. Esimerkkinä palvelunestohyökkäyksistä muun muassa Osuuspankin palvelimiin kohdistunut hyökkäys, joka vaikutti pankkiautomaattien toimintaan niin, että niitä ei pystynyt käyttämään ja asiakkaat eivät saaneet nostettua rahaa pankkiautomaateilta (Kerkkäinen 2016). Myös Sonyn palvelimiin on kohdistunut hyökkäys, joka kaatoi yrityksen Playstation Network -palvelun. Playstation Network -palvelu mahdollistaa pelien pelaamisen verkossa. (Kiss 2014.) Tämän tyyppiset hyökkäykset ovat hyvin kalliita yrityksille. Jotkut yrittävät arvioida yritykselle näistä koituneita kustannuksia ja summat liikkuvat kymmenissä tai sadoissatuhansissa euroissa per tunti, jolloin palvelimet eivät ole toiminnassa. (Saarelainen 2016.)

IoT (Internet of Things), eli esineiden internet tai teollinen internet nostaa tietoturvan tärkeyttä entisestään. Tavalliset ihmiset ostavat laitteita, jotka kytketään internetiin. Laitteet voivat hakea internetistä sovelluksia, laitteen käyttäjä voi selata tällä verkkosivuja tai laite kerää tietoa esimerkiksi käyttäjän ranteesta ja siirtää tiedon pilvipalveluun. Tietoturvayritykset näkevät tässä paljon mahdollisuuksia erilaisten tietoturvaohjelmien myymisessä.

Esineiden internet ei ole kuitenkaan uusi aihe tietotekniikan alalla. Esimerkiksi asuintaloissa on ollut etäluettavia vesi- ja sähkömittareita jo monta vuotta. Esineiden internet -aiheesta on kuitenkin vasta alettu puhumaan viimeisen parin vuoden aikana, jolloin kuluttajille vihjattiin esimerkiksi verkkoon liitettävästä jääkaapista ja pesukoneesta. (Brandom 2016.)

Puettavat elektroniset laitteet älykellojen ja urheilukellojen muodossa ovat tänä päivänä hyvin suosittuja (Tivi 2016). Älykellot kommunikoivat internetiin puhelimen tai tietokoneen avulla tai jopa suoraan, jonka takia nekin lukeutuvat esineiden internetiin. On uuti-

soitu esimerkiksi, että eri valmistajien, kuten Fitbit ja Garmin -älykellot pystyisivät käyttäjän tietämättä lähettämään käyttäjän terveystietoja ja sijaintitietoja hyökkääjälle, vaikka käyttäjä ei olisi antanut lupaa (Zeman 2016).

Markkinoille tulleet smart TV:t, joilla pystyy käyttämään suosittuja suoratoistopalveluita valtaavat jo kuluttajien olohuoneita. Samsungin smart TV:t ovat olleet huonossa valossa mediassa niiden tietoturvahaavoittuvuuksien takia. On kerrottu, että Samsungin smart TV pystyy kuuntelemaan sinua, vaikka et niin edes haluaisi. Tosin tämä ongelma on Samsungin mukaan korjattu. (Matyszczyk 2015.)

Teollinen internet, joka on sidonnainen esineiden internetin kanssa, on myös kovassa nosteessa. Yritykset pyrkivät parantamaan omaa liiketoimintaa erilaisilla älykkäillä koneilla, jotka keräävät tietoa yrityksille. Muutamalla suurella yrityksellä, muun muassa Microsoftilla (2017) ja IBM:llä on tiedon keräämiseen ja analysoimiseen soveltuvat ohjelmistot (IBM 2017). Dataa pyritään käyttämään omaan hyötyyn tai myymään sitä eteenpäin (IoT Finland 2015).

Teollinen internet on niin suuri asia tällä hetkellä, että sitä viitataan uuteen teolliseen vallankumoukseen. (Collin & Saarelainen 2016, 33.)

Työn tarkoituksena on käydä läpi esineiden internet -käsitteitä, miten IoT-tietoturvaongelmat pitäisi ratkaista, onko IoT-järjestelmiä mahdollisuus saada turvallisemmaksi erilaisten tietoturvaohjelmien ja -laitteiden avulla ja minkälaisia tuotteita markkinoilla on IoT-tietoturvan parantamiseksi kotiverkossa.

Tutkimusmenetelmänä on käytetty kvalitatiivista menetelmäsuuntausta.

2 ESINEIDEN INTERNET

Tässä luvussa esitellään esineiden internet -peruskäsitteitä, mitä se on ja miten se ilmenee normaalissa elämässä ja teollisuudessa.

2.1 Internet of Things

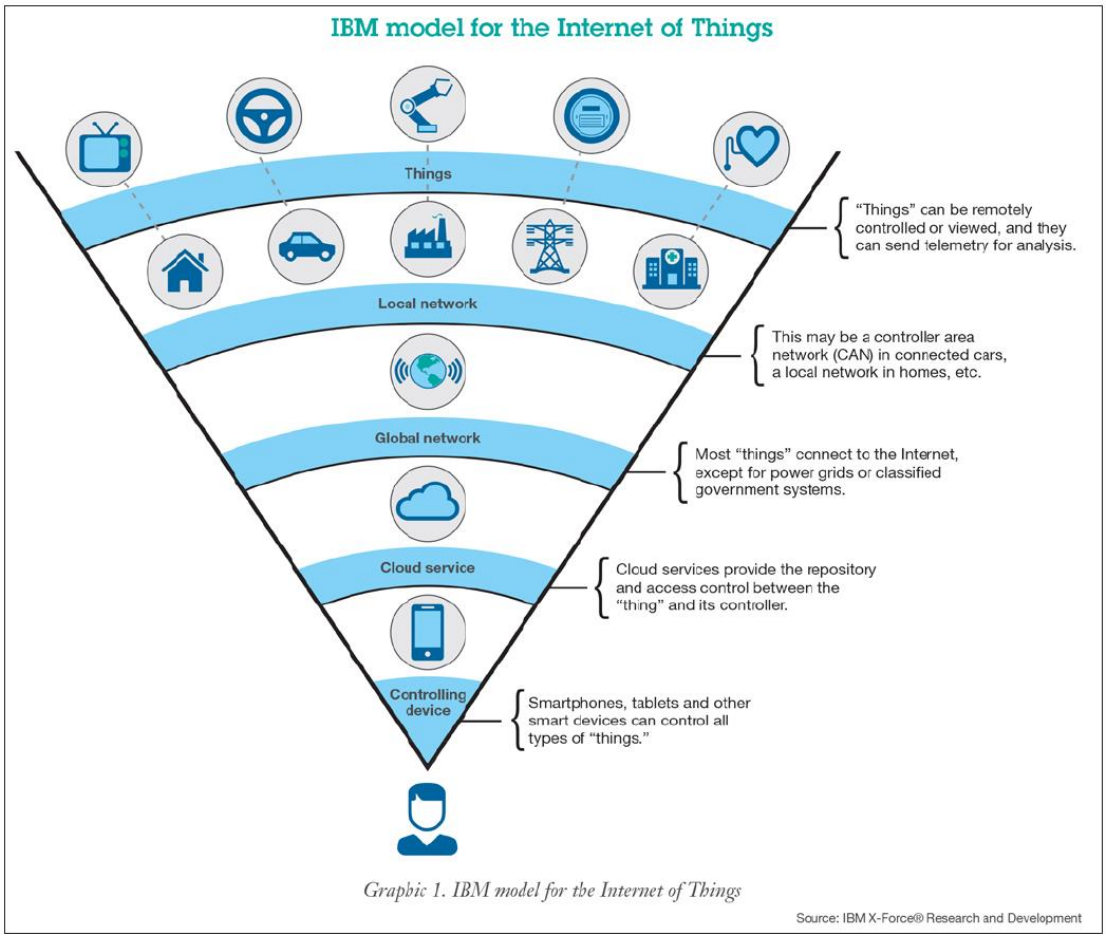
Internet of Things, eli esineiden internet on käsite, jolla tarkoitetaan verkon laajentumista laitteisiin, joita ei ole ennen kytketty internetiin. Nämä laitteet ovat yleensä jo olemassa olevia laitteita joihin lisätään verkkoyhteys ja antureita. Antureiden ja verkkoyhteyden avulla laite voi kerätä tietoa laitteen käytöstä tai laitteen ympärillä olevasta ilmastosta ja lähettää kerätty tieto verkkoyhteyden avulla esimerkiksi pilvipalveluun tai muihin laitteisiin. Tietoa voidaan analysoida eri tarkoituksiin. Analysointi voi tapahtua esimerkiksi internetistä selaimen avulla, jonka avulla pääsee käsiksi web-sovellukseen, johon laite on kytketty. Tai sovellus voi itse analysoida datan ja erinäisten laskelmien avulla päätellä esimerkiksi laitteen huollon tarvetta. Laite voi olla esimerkiksi jäteastia, joka sensorien avulla seuraa astian täyttyvyyttä ja lähettää siitä tietoa internetiin luettavaksi ja analysoitavaksi tai kotiverkossa oleva jääkaappi, joka videokameran avulla näyttää jääkaapin sisälle mitä jääkaapissa on. (Taanila 2016.)

Kuluttajalle esineiden internet voi tarkoittaa etäluettavaa lämpömittaria tai internetiin kytkettyä älytelevisiota. Valmistajat, kuten August ja Philips ovat tuoneet markkinoille älylukkoja, älyvaloja ja asunnon lämmityksen ohjauslaitteita, joihin on lisätty älyä (August 2017). Kuluttajalle esineiden internet pyrkii helpottamaan arkielämää, kuten älykellolla. Älykello voi esimerkiksi laskea käyttäjän askeleita ja tallettaa tämä tieto internetpalveluun, josta käyttäjä voi katsoa omia päivittäisiä askelmääriä. Kuluttajille suunnattu IoT on yleensä kytköksissä älykotiin. Älykodilla pyritään helpottamaan asukkaiden arkea esimerkiksi puhelimen sovelluksella ohjattavilla älylukoilla tai -valoilla. Erikoisimpia esimerkkejä esineiden internetistä on älyleivänpaahdin tai älyhiuskampa. (Philips 2017.)

Laitteet voivat olla yhteydessä muihin laitteisiin esimerkiksi lyhyen kantaman protokollilla, kuten Bluetooth, 6LoWPAN tai Zigbee. Kotiverkossa IoT-laitteiden kytkemiseen WLAN (Wireless Local Area Network) -verkkotekniikka on suosituin tapa yhdistää laite kotiverkkoon. WLAN on langaton verkkotekniikka, millä pystyy muodostamaan yhteyden

laitteiden välille langattomasti (Rouse 2010). Laitteet voivat käyttää myös suuren kantaman yhteyksiä, niin sanottua laajaa verkkoa, joita ovat 2G, 3G tai 4G LTE. (Collin 2016, 135.) On ennustettu, että IoT-laitteet kotona ovat tulevaisuudessa kytkettynä suoraan esimerkiksi valmistajan verkkoon käyttämällä viidennen sukupolven laajaa verkkoa 5G (IBM 2015).

IBM on tehnyt kuvan (kuva 1) kuluttajan näkökulmasta, miltä esineiden internet näyttää ja miten tieto kulkee ihmiseltä laitteeseen tai toisinpäin. IoT-laitteet ovat yhteydessä johonkin pilvipalveluun, johon laite kerää dataa. (IBM 2015.)



Kuva 1. Esineiden internet ihmisestä katsoen (IBM 2015).

2.2 Teollinen internet

Teollisella internetillä tarkoitetaan älykkäitä laitteita ja järjestelmää, mitkä keräävät tietoa sensorien avulla ja ovat yhteydessä internetiin tai toisiinsa, ja tällä pyritään esimerkiksi parantamaan tuotantoprosesseja ja liiketoimintaa. (Collin 2016, 25.)

Teollisen internetin avulla yritykset pystyvät analysoimaan tietoa, jotka laitteet ovat sensorien avulla kerännyt. Laite voi olla esimerkiksi kerrostalon hissi, johon on lisätty älykkyyttä, joka kerää automaattisesti tietoa omista osista tai toiminnoista ja tämän tiedon avulla ohjelma osaa sanoa, koska jokin osa täytyy vaihtaa tai hissi huoltaa. Tämä esimerkiksi helpottaa huomattavasti hissien huollon ajoittamista. Tästä on myös apua kotiverkon IoT-laitteiden kanssa. Esimerkiksi jääkaapissa voisi olla anturi mikä pitää lukua jääkaapin sisällä olevista tavaroista ja kun jokin tavara on loppumassa tai loppunut, jääkaappi voi itse tilata täydennystä tai lisätä puuttuvan tavaran listalle, josta näkee puuttuvat tavarat. (Plattonen 2015.)

Teollista internetiä pyritään hyödyntämään monilla eri aloilla. Terveydenhuollon puolella teollista internetiä on hyödynnetty liikutettavien potilassänkyjen ja lääkintälaitteiden paikannuksella. Sänkyihin ja lääkintälaitteisiin on laitettu rfid-tagi, joka on yhteydessä sairaalan rfid -antennijärjestelmään. Tähän järjestelmään kytketty ohjelmisto pystyy paikantamaan rfid-tagilla varustetut laitteet sairaalan sisätiloista. Tällä tekniikalla pystytään muun muassa paikantamaan huollon tarpeessa oleva laite. (Collin 2016, 83.)

Teollinen internet eroaa esineiden internetistä ainoastaan sillä, että termillä on helppo erottaa teolliseen tarkoitettua systeemiä kuluttajalla tarkoitetusta systeemistä (esineiden internet). Pääsääntöisesti nämä käsitteet kuitenkin tarkoittavat samaa. Kuluttajalla ja teollisuudella on kuitenkin eri päämäärä tiedon käyttämisen suhteen. Teollisuudessa tietoa kerätään oman liiketoiminnan hyväksi ja kuluttajille tarkoitetulla laitteella pyritään helpottamaan arkielämää.

Teollisen internetin kuin myös esineiden internetin on mahdollistanut elektroniikan hintojen laskun. Datan tallennus on helpottunut muun muassa sillä, että iso määrä tietoa mahtuu todella pieneen fyysiseen kokoon, internet on jokaisessa paikassa käytössä ja kehittyy koko ajan ja anturit pienentyvät ja paranevat toiminnallisesti. (Collin 2016, 35.)

Teollisen internetin päämääräksi voisi sanoa autonomisuus eli laitteet, jotka ohjaavat itse itseään ja toimivat kutakuinkin autonomisesti. Ihmiset halutaan pois esimerkiksi tuotantolinjoilta, että ihmisen tekemät inhimilliset virheet poistuisivat ja pystyttäisiin tekemään entistä tehokkaammin työtä.

IoT merkitsee kuluttajalle ja yrityksille aika eri asioita. Kuluttajan näkökulmasta katsoen haetaan IoT:llä ensisijaisesti sitä, että laitteet saadaan kytkettyä verkkoon ja hallittua sitä etänä. Yrityksille IoT on myös etähallintaa, mutta yrityksien kiinnostuksen kohteena ovat laitteiden muodostama data, jota pyritään hyödyntämään.

2.3 Muita käsitteitä

IoT sisältää myös muita käsitteitä esineiden internet ja teollisen internetin lisäksi. Muita käsitteitä on esimerkiksi IIoT, Industrial Internet of Things, joka on synonyymi teolliselle internetille. (Collin 2015, 26.)

Internet of Everything, eli kaiken internet on Gartner -tutkimusyhtiön luoma termi esineiden internetille. Suurista yrityksistä ainoastaan Cisco käyttää sitä aktiivisesti. (Collin 2015, 28.)

3 IOT-TIETOTURVA

Esineiden internetissä tietoturva on todella laaja-alainen aihe. Esineiden internet laitteiden käyttöönotossa pitää ottaa huomioon monia erilaisia tietoturvauhkia. IoT-laitteeseen kohdistuu erilaisia uhkia, kuten laitteen hallitseminen ulkopuolisen toimesta tai tiedon varastaminen. Huonosti suunnitellut IoT-kommunikaatioverkot ja IoT-sovelluksiin liittyvät tietoturva-aukot ovat isoja uhkia tiedon varastamisen kannalta IoT-järjestelmissä. Jos jonkin näistä osa-alueista jättää huomioimatta, koko järjestelmän tietoturva on uhattuna. (IBM 2015.)

Täytyy muistaa, että mitään järjestelmiä on mahdoton saada sataprosenttisen varmoiksi, mutta mitä useampi osa-alue on otettu huomioon, niin sitä varmempi järjestelmä on. Tietoturva on iso hidaste IoT-tekniikan käyttöönotossa yrityksissä (Collin 2016, 43). IT ja tietoturva henkilöt ovat hyvin tietoisia IoT:n vaaroista, jonka takia heidän tiedollaan pystytään IoT-järjestelmistä tekemään tietoturvallisia. Hyvällä suunnittelulla ja toteutuksella käyttäen parhaita tietoturvatapoja, joita käydään tässä pääluvussa, saadaan järjestelmistä hyvin tietoturvallisia.

Yksi suuri ongelma esineiden internetissä on se, että valmistajat haluavat mahdollisimman nopeasti mukaan valloilla olevaan trendiin näin laiteohjelmistoista tulee huonosti suunniteltuja ja toteutettuja tietoturvan kannalta. (DEFCONConference 2014.)

Toisenlainen ongelma on teollisuuden tulo IoT-maailmaan. Teollisuudessa on hallintajärjestelmiä ja laitteita, joita ei ole suunniteltu yhdistettäväksi verkkoon. Järjestelmät ja laitteet sisältävät vanhaa ja turvatonta tekniikkaa, mikä voi vaarantaa koko järjestelmän tietoturvan, jos tällainen laite tai järjestelmä kytketään verkkoon. Sama pätee kotiverkon IoT:hen. Halu kytkeä laitteita internetiin, joita ei ole ikinä sinne kytketty, lisää hyökkäyspintaa ja täten vaarantaa tiedon vuotamista ulkomaailmaan tai lisää mahdollisesti salakatselun mahdollisuutta. (Collin 2016, 188.)

IBM on jakanut esineiden internetin tietoturvan kahteen pääalueeseen. Makers of things, eli järjestelmän tietoturvasuunnittelu ja Operators of things, eli järjestelmien turvallinen käyttö. IBM (2015) on jakanut pääalueet näin:

Makers of things

- Tietoturvasuunnittelu

- Yksityisyydensuojan suunnittelu
- Tietoturvatestaus
- Jatkuva toimitusmalli
- Eheyden varmistaminen valmistuksessa ja toimittamisessa.

Operators of things

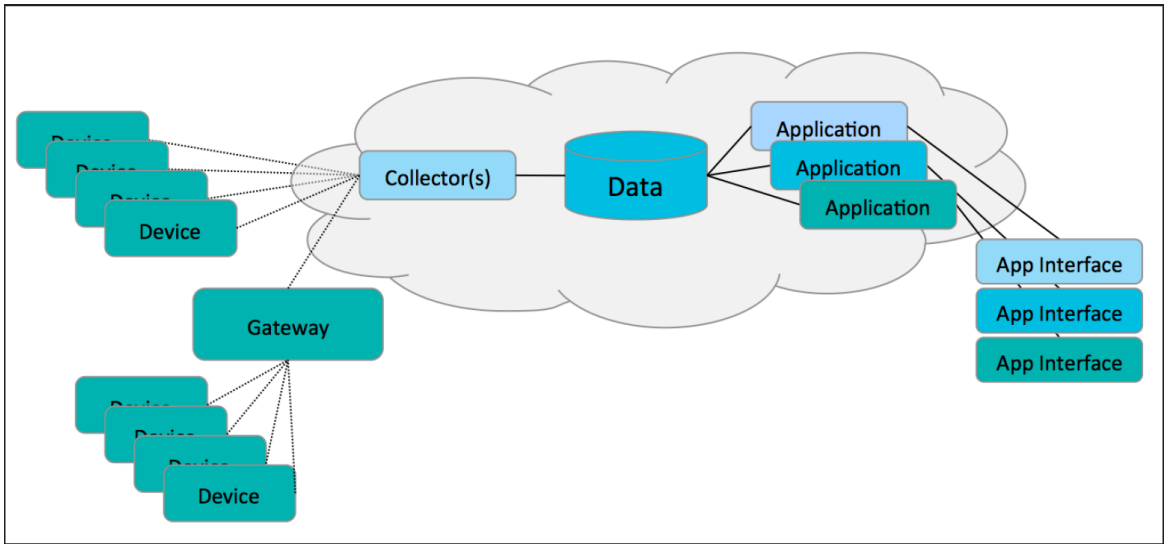
- Laitteen hyökkäyspinta-alan minimointi
- Laitekommunikaation salaus
- Laitteen toiminnan monitorointi
- Ylläpitää ajantasaista turvallista järjestelmää
- Muodosta luotettava huoltoekosysteemi.

Seuraavissa luvuissa käsitellään IBM:n dokumentin sisältöä ja tekstistä on valittu pääasiat tukemaan kotiverkon IoT-tietoturva-aihetta. Tämän dokumentin tukena on käytetty Open Web Application Security Project (OWASP) Top 10 IoT -projektin hyväksi katsomia toimia IoT-järjestelmän turvaamiseksi.

3.1 Monitasoinen tietoturva

Jokaiseen esineiden internet -järjestelmään tietoturva pitäisi toteuttaa niin sanotulla monitasoisella tietoturvalla (defence in depth). Monitasoisella tietoturvalla tarkoitetaan sitä, että järjestelmään on lisätty tietoturvaa parantavia puolustusmekanismeja eri järjestelmän kohtiin. Tämän tarkoituksena on varmistaa järjestelmän tietoturva, jos jokin tietoturvaa parantava osa ei toimi. Järjestelmän eri osille, kuten laitteelle, laiteohjelmalle ja laitteen ja pilven väliseen kommunikointiin on implementoitu eri tietoturvasuojia. (IBM 2015.)

IBM:n esineiden internet -järjestelmän kuva (kuva 2) havainnollistaa hyvin, mitä kaikkia osa-alueita esineiden internetissä pitää pitää mielessä, kun IoT-järjestelmän tietoturvaa suunnitellaan. Ilman jokaisen osa-alueen huomioon ottamista jo yksi tietoturvaongelma jollain osa-alueella voi vaarantaa koko järjestelmän tietoturvan. Esimerkiksi huonolla tietoliikenteen salauksella hyökkääjä voi poimia tietoliikenteestä käyttäjätunnuksen ja salasanan ja niillä tunnistautua järjestelmään varastetuilla tunnuksilla.



Kuva 2. Esineiden internet -järjestelmäkaavio (IBM 2015).

3.2 IoT-laitekommunikaation salaus

Laitekommunikaatioon voidaan käyttää monia eri yhteysprotokollia. Yleisimpiä IoT-laitteiden yhteydenmuodostustapoja toiseen laitteeseen tai järjestelmään, ovat tavallinen ethernet-yhteys, WiFi, ZigBee ja Bluetooth. (Collin 2016, 134.) Bluetooth Low Energy on pienen kantaman langaton yhteys, jonka hyötynä IoT:ssä on sen pieni virran kulutus ja 128 bitin AES-salaus (Collin 2016, 135).

Laitteiden yhteys toiseen laitteeseen tai internetiin täytyy salata. Liikenteen salaus voidaan toteuttaa Transport Layer Security (TLS) -tiedonsiirtosalauksella. TLS on paljon käytetty salausmetodi, joka salaa laitteiden välisen kommunikoinnin. Salaus on prosessi, jolla tehdään selkotekstistä salatekstiä, jota ei pysty lukemaan kuin osapuoli, jolla on jokin tapa tai avain salatekstin purkamiseen takaisin selkotekstiksi. (OWASP 2014a.)

Kommunikoinnin salaus IoT-järjestelmissä on tärkeää, ettei hyökkääjä voi kaapata laitteiden välillä siirrettävää tietoa ja käyttää sitä omaksi hyödykseen tai hyökkääjä pääsee käsiksi yhteyden väliin ja vaihtaa toiselta laitteelta tulevaa tietoa ennen kuin se saapuu toiselle laitteelle. (IBM 2015.)

Laitteiden tiedonsiirtoon käytetään monia erilaisia protokollia. Laitteet joille on annettu IP-osoite, pystyvät ne kommunikoimaan turvallisesti esimerkiksi TCP/IP (Transmission

Control Protocol / Internet Protocol) protokollan avulla, jonka päällä toimii TLS-salausprotokolla. TCP/IP protokolla mahdollistaa helpon TLS-salauksen. Muita kommunikaatioprotokollia ovat muun muassa paljon käytetyt MQTT (Message Queue Telemetry Transport) tai ModBus, joka on teollisuudessa teollisen internetin tiedonsiirron standardi. Kumpikin näistä protokollista pystyy käyttämään TCP/IP protokollaa. (Collin 2016, 145–147.)

Yritykset, jotka ylläpitävät IoT-järjestelmää, johon voi kuulua esimerkiksi pilvipalvelu, erilaiset tietokannat, toiminnanohjausjärjestelmä ja muita taustajärjestelmiä tiedonsiirron salaus voidaan toteuttaa VPN-yhteydellä. VPN eli virtual private network on yksityisen verkon laajentamista julkisen verkon yli niin sanotulla tunnelilla. Yritys pystyy esimerkiksi luomaan salatun yhteyden IoT-laitteeseen ja keräämään laitteesta anturin muodostaman datan pilvipalveluun analysoitavaksi turvallisesti. (Collin 2016, 56.)

3.3 Laiteohjelmiston tietoturva

Jokainen laite sisältää oman laiteohjelmiston eli firmwaren. Laiteohjelmisto huolehtii laitteen perustoiminnoista. Laiteohjelmistoon ei kuulu tallettaa salasanoja tai muuta herkkää tietoa, joka altistaisi laitteen tai ohjelmiston haavoittuvuuksille. Mikäli laiteohjelmistossa havaitaan virheitä, laiteohjelmisto tulisi päivittää. (IBM 2015.)

Vaikka laiteohjelmiston eheys, eli mahdollisten virheiden eliminoiminen laiteohjelmistosta on tärkeintä, laiteohjelmiston päivitys on ollut monen tietoturvasiantuntijan huolenaihe. ABI research -asiantuntijat ovat arvioineet vuonna 2013, että laitteita, joita kytketään internetiin, tulee olemaan 30 miljardia vuonna 2020 (ABI research 2013). Arviot kuitenkin heittelevät yritysten välillä. Tutkimusyhtiö Gartner arvioi, että laitteita tulee olemaan vuoteen 2020 mennessä 20 miljardia kytkettynä internetiin (Collin 2016, 18). IBM ehdottaa päivitystavaksi niin sanottua ”Over the air” -päivittämistä, joka tarkoittaa sitä, että päivityspaketti menee internetverkon yli laitteelle. Verkon yli päivittämisessä tulee ottaa huomioon, että hyökkääjällä on mahdollisuus päästä käsiksi päivityspakettiin, tai yhteyteen jossa tämä päivitys kulkee. Tätä varten päivityspaketin ja yhteyden tulisi olla vahvasti salattu, ettei hyökkääjä pääse muokkaamaan sitä. (IBM 2015.) Esimerkiksi Microsoft Azure IoT hub -ohjelmiston avulla pystyy päivittämään ohjelmistoon kytkettyjen laitteiden laiteohjelmisto etänä (Microsoft 2017).

IBM ehdottaa valmistajien sisällyttävän laitteeseen ”kill switch” ominaisuuden, joka tarkoittaa sitä, että kun laite on niin vanha, ettei sitä kannata enää päivittää jokaista hyökkäystä vastaan, laite olisi helppo eristää internetistä. Laite toimisi kuitenkin normaalisti, mutta ei kommunikoisi ulkoverkkoon. (IBM 2015.)

3.4 Ohjelmistojen turvallisuus

Laiteohjelmistojen turvaamisen lisäksi tarvitaan myös mahdollisten muiden sovellusten tietoturvaa, kuten web-sovelluksien turvallisuutta. Web-sovellukset ovat olleet jo kauan tietoturva alalla puheen aiheena ja niistä tiedetään jo paljon verrattuna esineiden internetin järjestelmän turvaamiseen. Maailmalla on esimerkiksi OWASP, joka on tehnyt vuodesta 2001 saakka web-sovelluksien turvaamiseksi töitä. OWASP on listannut Top 10 tietoturvauhkaa web-sovelluksia vastaan ja tätä käytetään usein perustana web-sovelluksien tietoturvahyökkäyksiä ja haavoittuvuuksia vastaan. (OWASP 2013.)

Muita ohjelmistoja, joita IoT-järjestelmään voi kuulua ovat esimerkiksi mobiilisovellukset. Mobiilisovellukset ovat isossa roolissa muun muassa kuluttajan IoT-laitteiden hallinnassa. (F-Secure 2016.) Mobiilisovelluksien turvallisuuteen kuuluu samoja tietoturvariskejä kuin web-sovelluksiin. Riskeihin lukeutuu muun muassa huonosti toteutettu tiedonsiirron salaus ja mobiililaitteeseen tallennetun tiedon huono salaus, joka johtaisi tiedon varastamiseen. (OWASP 2016.)

3.5 Käyttäjien ja laitteiden tunnistus ja todennus

Niin kuin muihin järjestelmiin tarvitaan turvallinen käyttäjien todennus, sitä tarvitaan myös esineiden internet järjestelmiin. Ilman hyvää ja turvallista käyttäjätodennusta ja valtuutuksia, kuka vaan voisi päästä muuttamaan tietoja ja poistamaan laitteita verkosta. Myös laitteet itsessään tarvitsevat jonkinlaisen tunnistuskoodin, jolla laite yhdistetään taustapalveluun. Suorin tapa on kytkeä laite kotiverkon turvalliseen langattomaan verkkoon esimerkiksi laitteen mukana tulleella tunnistuskoodilla, jonka avulla laite yhdistetään web-sovellukseen ja sitä kautta laite yhdistetään langattomaan verkkoon. Kun laite on yhdistetty langattomaan kotiverkkoon, pystyy laite yhdistymään internetiin esimerkiksi valmistajan pilvipalveluun valmistajan omalla laitteen ja pilvipalvelun tunnistuksella.

IoT-järjestelmät sisältävät monia eri alustoja, joihin käyttäjien tarvitsee päästä käsiksi. Yhteen järjestelmään voi kuulua web-applikaatio, pilvipalvelu ja mobiilikäyttöliittymä. Tämän lisäksi myös laitetta täytyy päästä hallitsemaan. Riittävä käyttäjätodennus tulisi sisältää ainakin nämä osa-alueet:

- vahva salasana
- salasanat eivät kulje verkon yli luettavassa ”clear text”-muodossa
- kaksiosainen todennus, jos mahdollista
- tärkeimpiin asioihin uudelleen todennus
- salasanan uusiminen on turvallista. (OWASP 2014b.)

Esimerkkinä huonosta käyttäjätunnus- ja salasanapolitiikasta, jossa salasanan vahvuus oli huono, on lokakuussa 2016 tapahtunut Mirai DDoS hyökkäys nimipalvelyhtiö Dyn palvelimille. Nimipalveluyhtiö on yritys, joka ylläpitää DNS-palvelimia, jotka muuttavat tietokoneiden ymmärtämän numeraalisen verkko-osoitteen ihmisten helposti muistettavaksi osoitteeksi ja toisinpäin. Mirai on haittaohjelma, joka etsii verkosta Linux-käyttöjärjestelmällä olevia laitteita, joiden Telnet-yhteydenmuodostus protokolla on auki ja yhteyden muodostuksen jälkeen kokeilee käyttäjätunnus ja salasana kombinaatioita, mitkä ovat helposti arvattavissa tai ovat tehdasasetettuja, esimerkiksi käyttäjätunnus Admin ja salasana admin. Kun haittaohjelma on päässyt laitteeseen kirjautumaan sisälle, haittaohjelma ottaa vallan laitteesta ja laitteesta tulee näin ”botti”, joka on osa saastuneiden laitteiden verkostoa. Hyökkääjä pystyy antamaan käskyn botille, esimerkiksi lähettämään pyyntöjä palvelimelle. Kun näitä pyyntöjä tulee miljoonista laitteista samaan aikaan, eikä palvelin pysty käsitellä tietomäärää, palvelin kaatuu ja sille ei pysty tehdä pyyntöjä. Tätä hyökkäysmuotoa kutsutaan palvelunestohyökkäykseksi eli DDoS. Tällä tavalla, kun Dyn-nimipalveluyhtiön palvelimille hyökättiin, monen suositun internetpalvelun käyttö loppui muutamiksi tunneiksi, koska monet sivustot käyttävät nimipalveluyhtiö Dynin DNS-palvelimia, jotka eivät pystyneet hyökkäyksen aikana muuttamaan verkko-osoitteita. Mirai -haittaohjelma oli saanut hyökkäykseen mukaan tulostimia, IP-kameroita, reitittimiä ja vauvamonitoreja. (Kerola 2016.)

3.6 Monitorointi

Myös IoT-järjestelmät tarvitsevat data-analysointia omasta toiminnastaan. Pelkällä ennaltaehkäisyllä ei saada järjestelmistä ja laitteista tietoturvallisia, vaan järjestelmien val-

vonta erilaisilla monitorointitavoilla on yksi tapa ehkäistä tietoturvauhkia. Esimerkiksi aktiivisella monitoroinnilla on mahdollista ehkäistä tietovuotoja tai -murtoja. Järjestelmien toimintatapoja ja liikennettä tulisi analysoida ja etsiä sieltä anomalioita, eli poikkeamia ja jos järjestelmän toimintatavat muuttuvat radikaalisti ja järjestelmässä liikkuu ennen näkemätöntä liikennettä voi hyvin olla kyseessä hyökkäys järjestelmässä. (IBM 2015.)

Varsinkin kuluttajapuolelle on tullut ja on tulossa laitteita kuten Bitdefender BOX, joka monitoroi ja analysoi verkkoliikennettä, joka tulee reitittimeen tai menee reitittimestä ulos etsien liikenteen seasta merkkejä hyökkäyksistä.

Myös F-secure on tuomassa markkinoille Sense-paketin, johon kuuluu reititin ja ohjelmisto. Sense-reitittimen ja -ohjelman tarkoituksena on analysoida kaikki tuleva ja menevä liikenne kodin ja ulkopuolisen netin välillä F-Secure Security Cloud -pilvipalvelun avulla. Kun laite huomaa poikkeamia tai muuta epäilyttävää liikennettä, se ilmoittaa siitä käyttäjälle puhelimen sovelluksen avulla. (F-Secure 2016.)

4 TIETOTURVAA ERILLISILLÄ TUOTTEILLA

Kuluttajille suunnattuja esineiden internet -tietoturvatuotteita ei paljon ole vielä tullut markkinoille. Bitdefender BOX on yksi tuote, joka on suunnattu nimenomaan kuluttajille omien kotona olevien laitteiden turvaamiseen. Myös F-Secure on tuomassa tuotetta kodin IoT-laitteiden tietoturvan parantamiseksi.

Seuraavissa luvuissa kerrotaan kuinka nämä kyseiset tuotteet sen tekevät.

4.1 Bitdefender BOX

Bitdefender on vuonna 2001 perustettu romanialainen kyberturvallisuuteen keskittyvä yritys, jolla on tuotteita niin yksityiskäyttöön kuin yrityskäyttöön. Yritys sanoo turvaavansa tällä hetkellä yli 500 000 000 henkilöä ympäri maailmaa. Bitdefenderillä on tuotteita kokonaisvaltaiseen kodin tietoturvasuojaukseen, johon kuuluu tietokoneiden ja mobiililaitteiden suojaus, ja tietoturvatuotteita, jotka suojaavat muun muassa ransomware-haittaohjelmilta ja niin sanottuja nolla-päivä -haavoittuvuuksia vastaan. Tässä luvussa käydään Bitdefenderin BOX -tuotteen ominaisuuksia läpi ja kuinka sillä pystytään parantamaan kodin IoT-laitteiden tietoturvaa. (Bitdefender 2016.)

Bitdefender BOX -laite on suunniteltu suojaamaan tietokoneita, älypuhelimia ja IoT-laitteita kotiverkon sisällä. Laitteen voi kytkeä joko yksinään ulkoverkon ja kotiverkon väliin jolloin se toimii itsenäisesti reitittimen roolissa tai laitteen voi kytkeä myös reitittimeen ja näin se tuo tietoturvasuojaa kotiverkkoon. Olemassa olevan reitittimen vierelle kytkettynä, vanhasta laitteesta kytketään pois DHCP (Dynamic Host Configuration Protocol), eli ominaisuus, joka jakaa laitteille omat IP-osoitteet automattisesti ja BOX:in kytkeytyessä verkkoon se ottaa DHCP-palvelimen roolin. Laite muodostaa olemassa olevaan reitittimeen tai suoraan ulkoverkkoon kytkettynä uuden turvallisen langattoman verkon. Tuotteen mukana tulee myös mobiililaitteille tarkoitettu VPN, joka pystyy toimimaan älypuhelimen tietoturvan lisääjänä. Tällä tavalla esimerkiksi julkisten langattoman verkon käyttö muuttuu turvallisemmaksi, kun yhteys on salattu. (Bitdefender 2016.)

BOX skannaa kotiverkon sisällä olevia laitteita muutaman päivän välein. Skannaus tarkistaa laitteiden salasanojen pituuden, laiteohjelmistojen version ja etsii laitteista muita

haavoittuvuuksia, kuten muun muassa takaovia, jotka mahdollistavat laitteeseen hyökkäämisen. (Nadel 2016.)

Bitdefender BOX maksaa 199 dollaria ja siihen kuuluu vuoden palvelunkäyttöoikeus ja vuoden jälkeen laitteen käyttö maksaa 99 euroa vuodessa. Bitdefender BOX:ia ei ole saatavilla Suomessa. (Bitdefender 2016).

4.2 F-Secure Sense

F-Secure on kansainvälisesti erittäin tunnettu eurooppalainen tietoturvayritys, joka on toiminut Suomessa vuodesta 1998 lähtien. F-Secure on perustettu Suomessa ja tällä hetkellä yrityksellä on pääkonttori Helsingissä ja toinen konttori Oulussa. Yrityksellä on toimistoja jokaisessa maaosassa, kuten Aasiassa, Euroopassa, Pohjois-Amerikassa ja Etelä-Amerikassa. F-Securella on satatuhatta yritystä ja kymmeniä miljoonia kuluttaja-käyttäjiä ympäri maailmaa asiakkaina. F-Securella on tietoturvatuotteita kuluttajille, näitä tietoturvatuotteita ovat muun muassa virustorjunta, VPN ja nyt uutena tuleva Sense IoT-tietoturvapaketti. Yrityksellä on myös yrityksille suunnattuja tietoturvaohjelmistoja, joilla pystyy suojaamaan päätelaitteita ja verkkoliikenteen. F-Securen tutkimuspäällikkö Mikko Hyppönen on viime vuosina ollut hyvin aktiivinen IoT-tietoturvasta puhuja. (F-Secure 2016.)

F-Secure Sense on F-Securen IoT-tietoturvaratkaisu kodin IoT-laitteille. Senseä ei ole vielä saatavilla. Sense-pakettiin kuuluu laite, ohjelmisto ja mobiiliohjelmisto. Laite kytketään reitittimen ja kotiverkon laitteiden väliin. Toisin kuin Bitdefender Box, Senseä ei voi kytkeä yksinään ilman reititintä. Sense ja reititin muodostavat uuden turvallisen langattoman Wifi-verkon, johon kotona olevat laitteet kytketään. F-Secure Sense monitoroi tietoliikenteen F-Securen -pilvipalvelussa, joten Sense-laitetta ei rasiteta. F-Securen pilvipalvelu on nimeltään Secure Cloud, joka kerää tietoa tuntemattomista sovelluksista, web-sivustoista ja haitallisista sovelluksista. Data analysoidaan F-Securella ja tätä kautta parannetaan haitallisen liikenteen parempaa havaitsemista. F-Securella on myös mobiililaite-tietoturvaohjelmisto, joka toimii pilvipalvelussa ja näin ei rasita puhelimen laskentatehoa. (F-Secure 2016.)

F-Secure Sense tulee maksamaan 199 euroa, joka sisältää laitteen ja vuoden käyttöoikeuden. Vuoden jälkeen palvelu maksaa 8 euroa kuussa (F-Secure 2016).

Seuraavassa kuvassa näkyy, kuinka Sense sijoittuu kotiverkkoon. Sense-laitteen päällä oleva kuva pilvestä ja F-Securen logosta kuvastaa pilvipalvelussa Secure Cloud -järjestelmällä tehtyä verkon tapahtumien analyysiä.

Kuva 3. F-Secure Sense (F-Secure 2016).

4.3 Yhtäläisyydet

Molemmat tuotteet pohjautuvat aktiiviseen verkkoliikenteen monitorointiin. Monitoroinnilla pyritään löytämään verkkoliikenteestä merkkejä aktiivisesta hyökkäyksestä tai estämään tiedettyjä sivuja, jotka on profiloitu haitallisiksi sivustoiksi. Tuotteet toimivat siis kuin palomuurit tietynlaisena gatewaynä, mutta lisänä vain aktiivinen monitorointi, joka pyrkii aikaisempien hyökkäysprofilointien avulla tunnistamaan esimerkiksi DDoS hyökkäykset. Valmistajien mukaan kummatkin tietoturvalaitteet lupaavat tehdä samat asiat, kuten estää virukset ja haittaohjelmat. Näiden lisäksi yritykset lupaavat aktiivista verkkoyhteyden monitorointia epäilyttävää liikennettä vastaan, ja turvaa internet selailun esimerkiksi estämällä käyttäjää menemästä tietyille tunnetuille URL verkkosivuille tai ottamaan yhteyttä tiedettyihin haitallisiin verkko-osoitteisiin. Tuotteet suojaavat kaikki laitteet, jotka ovat kyt-

kettynä verkkoon. Kotiverkon laitteet ovat palomuurisuojauksen takana ja tuotteet estävät omien tietojen vuotamisen internetiin. Valmistajat sanovat, että tämän laitteen lisäksi et tarvitse muita tietoturvatuotteita.

IoT-laitteet kytketään uuteen turvalliseen langattomaan WLAN-verkkoon, tai jossain tapauksissa, missä laitteella ei ole langattoman verkon tukea voi IoT-laitteen tai tietokoneen kytkeä myös suoraan esimerkiksi Sense-laitteeseen.

Molempia laitteita hallitaan mobiilisovelluksen avulla. Mobiilisovellukseen esimerkiksi F-Securen tapauksessa tulee ilmoitus käyttäjälle, jos järjestelmä havaitsee verkkoliikenteessä epäilyttävää toimintaa.

Molempien tuotteiden valtti on se, että ne pystyvät suojaaman laitteet joille ei ole olemassa tietoturvaohjelmistoa. Laitteille kuten älytermostaateille tai älypalohälyttimille ei ole kehitetty omaa tietoturvaohjelmistoa.

Tuotteet eivät ole kuitenkaan mitään uusia keksintöjä. Monitorointia on käytetty verkon tietoturvan parantamiseen jo kauan yrityksissä ja muissa järjestelmissä. Esimerkkinä suosittu avoimen lähdekoodin Snort -tunkeilijan havaitsemisjärjestelmä, joka monitoroi verkkoliikennettä ja antaa ilmoituksen, jos se löytää verkkoliikenteestä hyökkäykseen viittaavaa liikennettä (Snort 2017). On myös muita monitorointijärjestelmiä, kuten DLP (Data Leak Prevention tai Data Loss Prevention) ja IPS (Intrusion Prevention System) (Nixu 2016). Monitorointi on tuotteistettu kuluttajaystävälliseen pakettiin nyt myös kotiverkon IoT-laitteille.

Suurin ongelma kuluttajien IoT-laitteiden kanssa on, että IoT-laitteet, joiden tarkoituksena on kytkeytyä verkkoon ja laitteisiin pitää päästä etänä muodostamaan yhteys, ovat hyvin haavoittuvaisia myös ulkopuolelta tuleviin yhdistämisyrityksiin. Haavoittuneessa laitteessa voi olla esimerkiksi Telnet-etäyhteys päällä, johon ei tarvitse erillisiä tunnuksia laitteen ja hyökkääjän tietokoneen välille yhteyden muodostamiseen. Niin F-secure kuin Bitdefender pystyy omalla tuotteellaan estämään IoT-laitteiden näkyminen ulkoverkkoon niin, että kun IoT-laite on skannattu haavoittuvuuksien varalta tietoturvaohjelmiston avulla, tietoturvalaitteet ilmoittavat, jos IoT-laiteeseen on mahdollista ulkopuolisen hyökkääjän muodostaa etäyhteys. Tämä ei kuitenkaan poista sitä tosiasiaa, että laitteet itsessään ovat edelleen haavoittuvaisia ja huonosti suunniteltuja laitteen tietoturvan kannalta, vaikka siihen eteen laitetaan laite, joka piilottaa nämä toiset laitteet näkyvistä. Sekä Sense, että BOX on tarkoitettu kuluttajille, jotka eivät näitä oletuskäyttäjänimiä ja sala-

sanoja osaa tai ymmärrä vaihtaa. (Nadel 2016.) Näkisin kuitenkin niin, että mitä enemmän esimerkiksi yhdellä yrityksellä on IoT-laitteita myynnissä, sen varmemmin yritys alkaa miettiä myös laitteiden tietoturvaa.

4.4 Muita kotiverkon IoT-tietoturvalaitteita

Markkinoilla on myös muita IoT-tietoturvaan kehitettyjä tuotteita. Yritykset kuten CUJO, DOJO Labs ja Luma ovat tuoneet omat tuotteensa markkinoille parin viimevuoden aikana. Luma-tuotetta mainostetaan langattoman kotiverkon yhteyden parantajana, mutta myös kotiverkon tietoturvan parantajana monitoroinnin takia (Luma Home 2016). Näistä mainituista tuotteista ainoastaan DOJO Labsin tuote ei ole vielä saatavilla (DOJO Labs 2016). Kukin tuote on hyvin samanlainen. Jokaiseen tuotteeseen kuuluu laite, joka liitetään kotiverkkoon, joko suoraan tai olemassa olevaan reitittimeen. Pakettiin kuuluu myös mobiilisovellus älypuhelimeen laitteen ohjaamista varten. (CUJO 2016.)

Tuotteita eriteltäessä ilmenee, ettei näillä ole juuri mitään eroa. CUJO ja DOJO laitteet eroavat siinä määrin, etteivät ne muodosta uutta langatonta verkkoa vaan ne toimivat ainoastaan palomuurina. Jokainen tuote lupaa aktiivista verkkoliikenteen monitorointia, viruksien ja haittaohjelmien torjuntaa ja haitallisten sivujen estämistä. Hinnoittelussa on jonkin verran eroja. CUJO-laite maksaa 99 dollaria ja sen päälle tulee kuukausittainen maksu, joka on 8,99 dollaria, jota ei kuitenkaan tarvitse maksaa kuin vasta 180 päivän jälkeen laitteen ostamisesta. Kuukausittaisella maksulla laitteen saa käyttöön. Laitteen mukana on myös mahdollista ostaa valmiiksi laitteen käyttöoikeus, jolla laitetta ja ohjelmia pystyy käyttämään aina ilman uusia maksuja: eli laitteen ostamisen jälkeen ei tarvitse maksaa edellä mainittua 8,99 dollaria kuussa. Laitteen saa käyttöön ilman muita maksuja 150 dollarilla. (CUJO 2016.)

DOJO Labs -laitteen saa 199 dollarilla ja siihen kuuluu 12 kuukauden palvelun käyttömahdollisuus (DOJO Labs 2016). DOJO Labsin -laitteen 12 kuukauden sopimuksen jälkeinen hinta ei ole tiedossa, kun taas Luma-laitteen saa käyttöön 149 dollarilla ja siihen päälle täytyy maksaa 14 dollarin kuukausittainen käyttöoikeus (Luma Home 2016).

Tuotteet ovat melko lähellä toistensa hintoja. Tietoturvaohjelmien puolella on ollut jo pitkään, että ohjelmiston käyttämisestä joutuu maksamaan vuosittaisia tai kuukausittaisia maksuja.

Näkisin, että rahojen sijoittaminen ei niin tunnettuihin tietoturvayrityksiin ja niiden uusiin tuotteisiin ei mielestäni ole kannattavaa. Suuremman ja tunnetumman yrityksen tuotteen ostaminen on järkevämpää jo sen takia, että suuremman yrityksen muut tietoturvatuotteet on testattu miten hyvin ne estävät esimerkiksi haittaohjelmien läpi pääsemisen tietokoneeseen tai verkkoon.

5 POHDINTA

IoT-järjestelmän tietoturvaan kuuluu monenlaisia ongelmia. Esimerkiksi IoT-laitteen ja ohjelmiston testaus on tärkeää tietoturva-aukkojen löytämiseksi. IoT-tietoturva aiheena on hyvin sekava, koska siihen liittyy niin monta eri osa-aluetta, kuten laite- ja ohjelmistoturvallisuus, jotka ovat laajoja aiheita. Tuotteista ei ole vielä tutkittua tietoa ja niiden aitoa toimivuutta ei ole vielä kunnolla testattu.

Yksi suurimmista uhista tietoturvallisuudelle on tällä hetkellä IoT. Palvelunestohyökkäyksillä on saatu aikaan isoja tuhoja, muun muassa pankkiautomaattien toiminnan pysäytys. IoT:n takia kokonaisen kerrostalon lämmitysjärjestelmiä on saatu ajettua alas. Mirai Botnet -hyökkäys tuli ilmi ja lähdekoodi on tällä hetkellä internetissä vapaassa jaossa. Tietoturvauutiset ovat liittyvät usein IoT:hen. F-Securen Mikko Hyppönen puhuu todella usein IoT:n vaaroista ja kuinka hän kauhuissaan odottaa, mitä IoT voi saada aikaan.

Kuluttajien IoT-laitteiden pitäisi pystyä olemaan turvallisempia. Tietoturva-alan asiantuntijoilta on tullut kommentteja IoT-tietoturvaan liittyen ja kommentit ovat olleet kaksijakoisia. Toinen puoli on sitä mieltä, että meillä on jo olemassa olevia tekniikoita laitteiden suojaamiseen ja niitä pitäisi osata soveltaa. Toinen puoli taas on sitä mieltä, ettei näillä menetelmillä selvitä IoT-maailmassa. Kuten aikaisemmin on käynyt selväksi, monitorointi ei ole uusi asia tietoturvapuolella. Monitoroinnin on havaittu toimivan tietoturvaa lisäävien tietoturvalaitteiden puolustusmetodina ulkopuolelta tulevien hyökkäysyritysten torjumiseksi. Tekniikka IoT-laitteiden turvaamiseksi kotiverkossa löytyy, mutta sen tuominen markkinoille kestää myös isoilla yrityksillä.

IoT:n kanssa onneksi ollaan vielä siinä tilanteessa, että yritykset eivät ole varmoja, kuinka ne pystyvät hyötymään IoT:n tuomista mahdollisuuksista. Näin myös tietoturvapuolella on enemmän aikaa löytää ratkaisu. Aikaa ei kuitenkaan ole paljoa, niin kuin esimerkiksi Mirai botnet -hyökkäys on antanut ymmärtää.

Vaikka minusta tuntuukin, että tällä hetkellä Sense tai BOX -laittet onkin tarkoitettu enemmän henkilöille, joille tekniikka on hyvin vierasta, voisin jopa itse tulevaisuudessa ajatella ostavani esimerkiksi F-Securen Sense tuotteen ja ainoastaan sillä turvata kotiverkkoni ja kotiverkon ulkopuolella puhelimeni VPN:n avulla. Jos IoT-laitteet yleistyvät sitä vauhtia mitä on uskottu, niin hyvin pian on todennäköistä, että jokaisella on saman tyyppinen laite kotona. Jos Sensen tapaiset laitteet alkavat yleistyä kuluttajien kotona ja todetaan,

että laite toimii ja siihen pystytään luottamaan tietoturvan näkökulmasta, on tämä hyvin iso asia IoT-laitteiden valmistajille. Valmistajien ei välttämättä tarvitse panostaa tuotteiden tietoturvaan niin vahvasti kuin esimerkiksi nyt. Tämä ei kuitenkaan ole valmistajan näkökulmasta mahdollista. IoT-tietoturvalaite antaa kuluttajalle luottoa verkon turvallisuudesta, mutta ei pienennä IoT-laitevalmistajien tietoturvasuunnittelutyötä. Totta kai valmistajalla on oma vastuu tietoturvapuolella ja eivät he voi olettaa, että kaikilla on Sensen kaltainen laite kotona. Esimerkiksi IoT-laitteen keräämä tieto pilvipalveluun on täysin valmistajan vastuulla, sitä ei BOX:in tai Sensen kaltainen laite pysty turvaamaan.

Oma pohdinnan alue on, pystyykö IoT-tietoturvaa parantavaan laitteeseen luottamaan ja laitteen valmistajayritykseen. Laite laitetaan kotiverkon ja ulkoverkon väliin, jolloin se analysoi kaiken läpi menevän datan. Käyttäjä kuka haluaa mahdollisimman paljon yksityisyyttä verkossa ei välttämättä halua, että erillinen laite kerää tietoa datasta, joka liikkuu ulkoverkon ja kotiverkon välissä. Esimerkiksi F-Secure on todennut, että heidän Secure Cloud -järjestelmänsä poistaa datasta kaikki yksilön identifioimiseen mahdollistava tieto, josta pystyisi identifioimaan datan alkuperän (F-Secure 2017). Vaikka tietoturvalaite suojaisi kotiverkkoasi, ei se takaa sitä, että olisit suojassa kaikilta hyökkäys- tai urkintayritykseltä.

LÄHTEET

ABI research 2013. Viitattu 17.11.2016. https://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne/

August 2017. Viitattu 16.11.2016. http://august.com/

OWASP Foundation 2014a. Top IoT Vulnerabilities. Lack of Transport Encryption. Viitattu 16.11.2016 https://www.owasp.org/index.php/Top_10_2014-I4_Lack_of_Transport_Encryption

OWASP Foundation 2014b. Top IoT Vulnerabilities. Insufficient Authentication/Authorization. Viitattu 17.11.2016 https://www.owasp.org/index.php/Top_10_2014-I2_Insufficient_Authentication/Authorization

OWASP Foundation 2013. OWASP Top Ten Project. Viitattu 17.11.2016. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=Main

OWASP Foundation 2016. OWASP Mobile Security Project. Viitattu 17.11.2016. https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_10_Mobile_Risks

Maras, M–H. 2015. Internet of Things: security and privacy implications. International Data Privacy Law, 99–04. Viitattu 19.10.2016 http://search.proquest.com.ezproxy.turkuamk.fi/docview/1704856770?accountid=14446

Norse 2016. Viitattu 19.10.2016. http://map.norsecorp.com/

Brandom, R. 2016. Samsung's fridge of the future will let you check spoilage from your phone. Viitattu 7.11.2016 http://www.theverge.com/2016/1/4/10707894/samsung-smart-refrigerator-connected-fridge-iot-ces-2016

Matyszczyk, C. 2015. Samsung's warning: Our Smart TVs record your living room chatter. Viitattu 7.11.2016 https://www.cnet.com/news/samsungs-warning-our-smart-tvs-record-your-living-room-chatter/

Microsoft 2017. Azure. Viitattu 19.10.2016. https://azure.microsoft.com/en-us/

IBM 2017. Watson Internet of Things. Viitattu 19.10.2016. https://www.ibm.com/internet-of-things/

IBM 2015. IBM point of view: Internet of things security. Viitattu 7.11.2016 http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=RAW14382USEN&attachment=RAW14382USEN.PDF

Taanila, I. 2016. Internet of Things (IoT). Viitattu 16.11.2016 http://iotfinland.fi/internet-of-things-iot/

Tivi 2016. Älykellojen suosio kasvussa – älylaseista tuskin tulee ihmeempää hittiä jatkossakaan. Viitattu 19.10.2016. http://www.tivi.fi/Kaikki_uutiset/alykellojen-suosio-kasvussa-alylaseista-tuskin-tulee-ihmeempaa-hittia-jatkossakaan-6250365

Philips 2017. Viitattu 16.11.2016. http://www.philips.fi/

Plattonen, J. 2015. IoT-datan käsittely ja ennustaminen. Viitattu 16.11.2016 http://iotfinland.fi/iot-datan-kasittely-ja-ennustaminen/

Rouse, M. 2010. Wireless LAN. Viitattu 16.11.2016. http://searchmobilecomputing.techtarget.com/definition/wireless-LAN

Collin, J. & Saarelainen, A. 2016. Teollinen internet. Helsinki: Talentum.

DEFCONConference 2014. DEF CON 22 - Mark Stanislav & Zach Lanier - The Internet of Fails - Where IoT Has Gone Wrong. Viitattu 16.11.2016 https://www.youtube.com/watch?v=WHdU4Lut-BGU

Kerkkäinen, T. 2016. Motiivina hillitön pätemisen ja rahan tarve – näin teinihakkerit kaatoivat OP:n verkkopankin. Viitattu 19.10.2016. http://yle.fi/uutiset/3-9258886

Kerola, P. 2016. Perjantain suuren verkkohyökkäyksen hurja tausta: Hakkerit valjastivat kodinkoneita aseikseen. Viitattu 17.11.2016 http://yle.fi/uutiset/3-9246350

Kiss, J. 2014. Xbox live and PlayStation attack: Christmas ruined for millions of gamers. Viitattu 19.10.2016. https://www.theguardian.com/technology/2014/dec/26/xbox-live-and-psn-attack-christmas-ruined-for-millions-of-gamers

IOT Finland 2015. IoT-datan analysointi ja hyödyntäminen. Viitattu 19.10.2016. http://iotfinland.fi/iot-datan-analysointi-ja-hyodyntaminen/

F-Secure 2017. Secure Cloudin yksityisyyskäytäntö. Viitattu 24.3.2017. https://www.f-secure.com/fi_FI/web/legal/privacy/security-cloud

F-Secure 2016. F-Secure Sense. Ominaisuudet. Viitattu 14.12.2016 https://sense.f-secure.com/fi/

Bitdefender 2016. Bitdefender BOX FAQ. Viitattu 14.12.2016 http://www.bitdefender.com/box/faq/

Nadel, B. 2016. Bitdefender Box Review. Viitattu 21.2.2017 http://www.tomsguide.com/us/bitdefender-box,review-3766.html

Cujo 2017. Cujo FAQ. Viitattu 9.2.2017 https://support.getcujo.com/support/home

DOJO Labs 2017. DOJO FAQ. Viitattu 9.2.2017 http://www.dojo-labs.com/product/faq/

Luma Home 2017. Luma Frequently Asked Questions. Viitattu 9.2.2017 https://support.luma-home.com/hc/en-us/categories/202886587-Frequently-Asked-Questions

Saarelainen, A. 2016. Dos-hyökkäys kaataa nettipalvelun – miten voin suojautua? Viitattu 19.10.2016. http://www.tivi.fi/Kaikki_uutiset/dos-hyokkays-kaataa-nettipalvelun-miten-voi-suojatua-6535679

Snort 2017. Snort FAQ. Viitattu 7.3.2017 https://www.snort.org/faq

Nixu Oyj 2016. Hyökkäyksen havainnointi- ja estojärjestelmät. Viitattu 8.3.2017 https://www.nixu.com/fi/palvelualueet/hy%C3%B6kk%C3%A4yksen-havainnointi-ja-estoj%C3%A4rjestelm%C3%A4t-ips-ids

Zeman, E. 2016. Fitbit, other fitness trackers leak personal data: study. Viitattu 19.10.2016. http://www.informationweek.com/mobile/fitbit-other-fitness-trackers-leak-personal-data-study/a/d-id/1324165